THE SIGNIFICANCE AND FUNCTION OF CYBERSPACE IN THE ADVANCEMENT OF THE DIGITAL ECONOMY

Rustamov Alisher Bahadirovich
Associate Professor, University of Information Technologies and Management
E-mail: alirus900@gmail.com

Abstract. As the business moves to digital and online models, risks are quickly outpacing traditional methods of protecting data. Governments and businesses are being challenged more than ever to be proactive in establishing and changing systems to protect against these dangers. This essay looks at how cyber risks affect the quickly growing digital economy.

Keywords: Digital economy, dangers, risk, privacy, information security, information, vulnerabilities, communication technologies, and possible risk are all important words.

Аннотация. Поскольку бизнес переходит на цифровые и онлайн-модели, риски быстро опережают традиционные методы защиты данных. Правительства и бизнес как никогда сталкиваются с вызовом быть проактивными в создании и изменении систем для защиты от этих опасностей. В этом эссе рассматривается, как киберриски влияют на быстрорастущую цифровую экономику.

Ключевые слова: цифровая экономика, опасности, риск, конфиденциальность, информационная безопасность, информация, уязвимости, коммуникационные технологии, возможный риск — все это важные слова.

Annotatsiya. Biznes raqamli va onlayn modellarga o'tishi bilan xavflar ma'lumotlarni himoya qilishning an'anaviy usullaridan tezroq oshib bormoqda. Hukumatlar va korxonalar ushbu xavflardan himoya qilish uchun tizimlarni o'rnatish va o'zgartirishda faol bo'lishlari har qachongidan ham ko'proq talabulosa. Biznes raqamli va onlayn modellarga o'tishi bilan xavflar ma'lumotlarni himoya qilishning an'anaviy uib chiqiladi.

Kalit so'zlar: raqamli iqtisodiyot, xavf, xavf, maxfiylik, axborot xavfsizligi, axborot, zaifliklar, aloqa texnologiyalari va yuzaga kelishi mumkin bo'lgan xavf-bularning barchasi muhim so'zlardir.

Introduction

Cybersecurity is now a vital and non-negotiable part of running a business in the digital economy. The word may sound easy, but it means more than just helping to keep our privacy and integrity safe and our digital assets and online presence safe. We all know what cyber security is and how important it is in today's fast-paced world of technology.

ISSN 3030-3907

The use of digital technology in the economic transformation might lead to new dangers and hazards as new technologies and functionalities become available in the digital economy. Governments must identify potential risks and hazards as implementers and regulators of the economy in order to protect the national economy during the digital economic transition. The quality and correctness of the policy that was put into place will determine how well the steps taken to reduce risks and threats to national economic security work. A thorough analysis of the risks and vulnerabilities provided by cyber threats in the digital economy is important. This should include all economic activities, especially the relationships between the people who are participating in the economic process.

A cyber security threat is any bad action that tries to damage, steal, or mess up data, important systems, or digital life in general. Some of these hazards are computer viruses, malware attacks, data corruption, and denial of service (DoS) attacks. These cyber security dangers have changed as we rely more on technology, making them more dangerous for people and enterprises. The first step to staying safe from cyber attacks is to know what they are.

There are many different persons, places, and situations that pose cybersecurity dangers to the digital economy. Malicious cyber threat actors can be:

Groups of criminalsOrganized hacker groups want to get into businesses to make money. Phishing, spam, spyware, and malware are all types of cyber threats that are used for extortion, identity theft, and online scams that work like businesses, with many people working together to plan and carry out assaults.

CountriesHostile countries can execute cyberattacks against businesses and organizations in their own country to disrupt communications, inflict chaos, and damage. An organization that is a terroristTerrorists use cyber attacks to damage or destroy important infrastructure, put national security at risk, hurt the economy, and hurt civilians. Insiders who liePeople who work for a firm and have legitimate access to its assets exploit that access to steal information or destroy electronic assets for their own financial or personal benefit. These dangers from inside the company can come from employees, contractors, suppliers, or business partners.

The economic cost of a security breach does not include indirect costs to victims, such as lost productivity, downtime, lost opportunities, brand stigma, loss of trust, intellectual property theft, and damage to employee morale. They also leave out systemic expenses, such how changes in the supply chain affect suppliers higher up and customers lower down.

As technology gets better, so are the ways that hackers try to take advantage of weaknesses for their own gain. Experts claim that cybercrime is the biggest danger to all businesses and industries. The globe has 200 zettabytes of data, which is the same as one trillion gigabytes or 1,000,000,000,000,000,000,000 bytes.

ISSN 3030-3907

Cybercriminals will keep going after this data since it is so valuable. The Center for Strategic and International Studies (CSIS) and McAfee say that cybercrime has the most effect on the economy in Europe, where it costs about 0.84 percent of GDP. In North America, cybercrime costs the economy 0.78% of the region's GDP. The World Economic Forum said that IoT devices were used in 1.5 billion attacks in the first half of 2021, which is 15% more than the same time last year. There are no rules for making IoT devices right now, therefore they are being used more quickly than before. This is made worse by onboard security, common setup problems, and the fact that these devices often link to networks over insecure wifi. We also look at how cyber assaults can have a big effect on people, including the emotional, financial, and mental effects that victims may experience in the chart below.

Loss of money and identity theftOne of the most direct and clear repercussions of cyber attacks on people is that they lose money. Hackers employ a lot of different ways to obtain private financial information, such as phishing scams, ransomware, and credit card fraud.

Hurt feelings and reputationsCyber attacks can potentially hurt someone's reputation and relationships. People can be blackmailed, embarrassed, or slandered through social engineering attacks or leaks of sensitive information. This can have a big impact on their personal and professional lives. After something like this, it can be hard to rehabilitate your reputation and regain the trust of friends, family, and coworkers.

Attacks that lock you out of your computer or hold your data for ransomWhen someone gets hit with ransomware or a denial-of-service attack, they may not be able to access important systems, which can slow down their work and make it harder to run their business. This can cause missed chances, lost money, and failure in both your personal and professional life.

Stress and effects on mental healthThe psychological effects of cyber attacks should not be ignored. People who have been hurt often feel more stressed, have trouble sleeping, and feel weak all the time. Knowing that cyber threats are always out there can make a person anxious all the time, which can hurt their mental and physical health.

Have faith in digital services and technologiesPeople may lose faith in digital services and technology as cyber attacks becoming more advanced. People who don't trust new technologies or online activities may not be able to fully enjoy the digital world.

These risks can be planned or unplanned, and they can cause data breaches, money losses, and damage to your reputation. To keep your computer safe, it's

ISSN 3030-3907

important to know about the many kinds of insider threats and how to deal with them.

Figure 1.

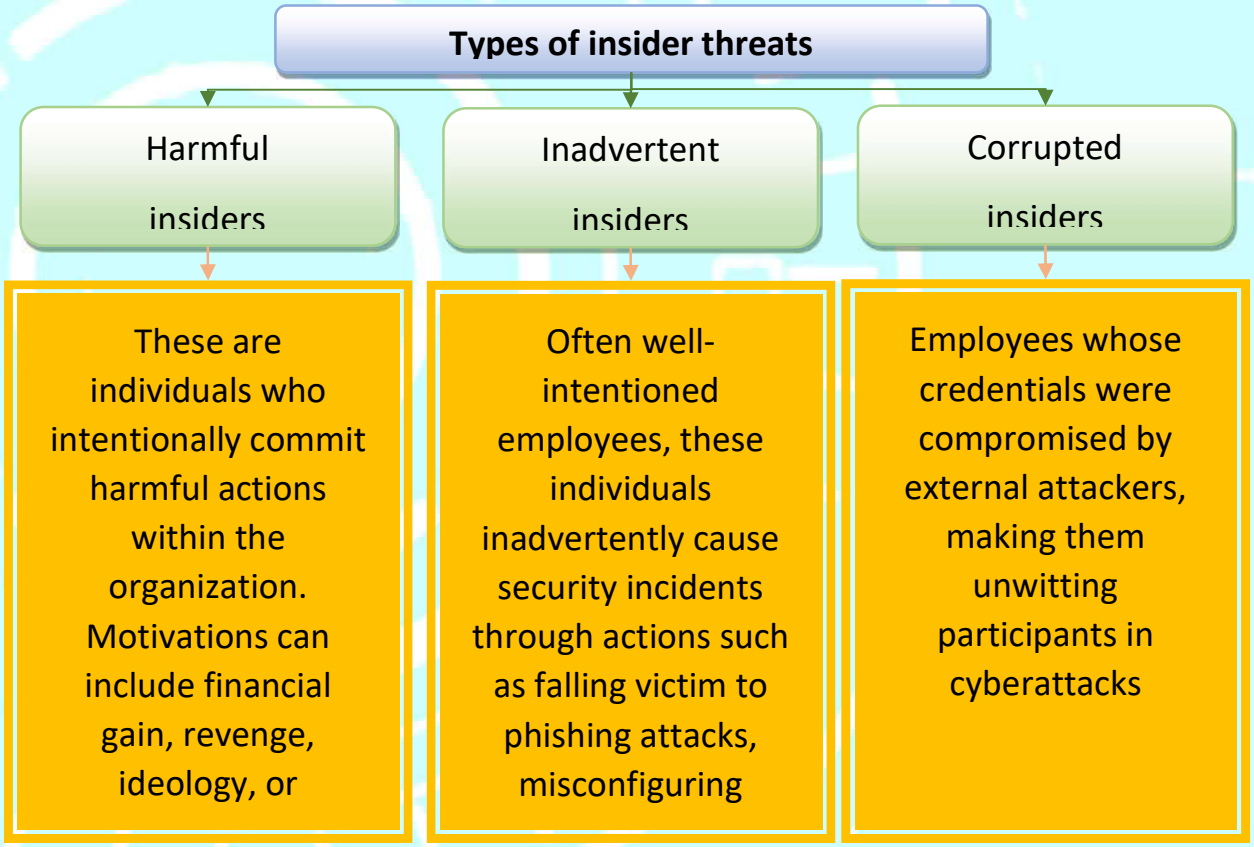


Figure 1. Different kinds of insider risks.

Cyberattacks have effects on people that go beyond the digital world. They can hurt their finances, mental health, relationships, and trust in technology. As we go into the digital age, it's important for people to be careful and take steps to secure their online presence. Following good cybersecurity practices, keeping up with the latest threats, and utilizing trusted security technologies can all help you avoid becoming a victim of cyberattacks.

Also, people, businesses, schools, and governments need to work together to fight cybercrime and make the internet safer for everyone. We can make the digital world safer and more stable by working together to deal with the problems that cyber threats cause. This will also protect everyone's privacy and health.

Conclusion

Cybersecurity is crucial in today's digital economy, where the transformation to online models raises significant risks. This essay discusses the growing threats posed by cybercrime, including attacks from malicious actors like criminal groups, hostile nations, and insiders. The financial and psychological impacts of cyber incidents on individuals and organizations are emphasized, detailing direct monetary losses, reputation damage, and mental health issues. The report highlights the increasing costs of cybercrime, particularly in regions like Europe and North

ISSN 3030-3907

America, and stresses the importance of collaborative efforts among stakeholders to enhance cybersecurity measures. Effective risk management, awareness, and maintaining updated security practices are essential for protecting digital assets and privacy in a rapidly evolving technological landscape.

REFERENCES

1. Kominfo. (2020). Infographic showing the digital transformation statistics for Indonesia in 2020. Jakarta: Infographics on the 2020 Digital Transformation Statistics in Indonesia.
2. Kuznetsova, M. A. (March 22, 2022). ndustry 4.0 Risks and Their Effect on Industrial Organizations - Economy: Issues, Remedies, and Future Outlook.
3. .The National Crime Agency (2020). Crime on the internet. The National Crime Agency got this on March 20, 2022: ttps://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
4. Piliang, Y. A. (2012). Digital and Information Society: Information Technology and Social Change. Jurnal Sosioteknologi, 155.
5. World Economic Forum. (2019). Fourth Industrial Revolution: Signs of Technology and New Ideas in Manufacturing. World Economic Forum at Cologny
6. Alisher, R., and Fayzi, B. are teachers in the Information Security department of the Karshi branch of TUIT. 2. SCIENTIFIC REPORTS OF BUKHARA STATE UNIVERSITY
7. Kadyrov, B. K. (2022). Problems and solutions in teaching the database in higher education (on the example of technical education). *current research journal of philological sciences*, *3*(07), 35-41.
8. Kadyrov, B. K. (2022). Perspectives of problems in the study of database science in the Credit-Module System and their solutions. *International Journal of Formal Education*, *2*(1), 16-22.
9. Shoniyozova, Y. Q., Turdiyeva, M. A., & Norboyev, B. U. (2020). NETWORK ATTACK PREVENTION SYSTEMS. *ИННОВАЦИОННЫЕ МЕХАНИЗМЫ И СТРАТЕГИЧЕСКИЕ ПРИОРИТЕТЫ НАУЧНО*, 46.
10. Bekhzod, N. (2023). DATA ANALYTICS MODEL IN LOAN APPROVAL PREDICTION. *Innovations in Technology and Science Education*, *2*(15), 262-269.
11. Zohirov, K., Temirov, M., Boykobilov, S., Berdiev, G., Ruziboev, F., Egamberdiev, K., ... & Madatov, K. (2025). Electromyography-Based Sign Language Recognition: A Low-Channel Approach for Classifying Fruit Name Gestures. *Signals*, *6*(4), 50.

ISSN 3030-3907